

智能车载网络中匿名认证与密钥交换协议^{*}

张晓均, 唐浩宇, 付红, 王文琛
(西南石油大学计算机科学学院, 四川 成都 610500)

摘要: 智能车载网络是实现智能交通系统的核心, 近年来受到学术界越来越多的关注, 但车载网络固有的开放性、脆弱性导致其面临许多安全问题。为解决智能车辆与附近 RSU 之间双向认证和会话密钥的交换以及智能车辆的身份匿名性问题, 提出智能车载网络中匿名认证与密钥交换协议。协议中设计了基于身份的数字签名算法, 使得智能车辆以身份完全匿名的方式向附近的路边基站单元发送认证信息。当路边基站单元通过认证之后, 计算一个消息认证码作为响应信息发送给请求认证的智能车辆, 以实现双向认证。此外, 在匿名认证的同时还能进行会话密钥的协商, 用于后续的安全保密通信。协议是基于身份密码系统设计的, 不需要复杂的证书管理。性能评估表明, 所提协议能够有效部署在智能车载应用场景。

关键词: 智能车载网络; 身份匿名; 密钥交换; 双向认证; 消息认证码

中图分类号: TP309

文献标志码: A

doi: 10.3969/j.issn.1007-130X.2024.01.009

Anonymous authentication and key exchange protocol in intelligent vehicle networks

ZHANG Xiao-jun, TANG Hao-yu, FU Hong, WANG Wen-chen
(School of Computer Science, Southwest Petroleum University, Chengdu 610500, China)

Abstract: Intelligent vehicular ad hoc networks (VANETs) are the core of intelligent transportation systems, in recent years, it has received increasing attentions from the academic community. However, due to the openness and fragility, VANETs are confronted with many security problems. In order to solve the problems such as two-way authentication between intelligent vehicles and nearby RSUs, exchange of session keys and anonymity of intelligent vehicles, this paper proposes an anonymous authentication and key exchange protocol in the intelligent vehicle networks. In the protocol, an identity-based digital signature algorithm is designed to enable the intelligent vehicle to send authentication information to the nearby road side unit (RSU) in a completely anonymous manner. After the RSU validates the authentication information, a message authentication code will be calculated and sent to the intelligent vehicle as the response to realize two-way authentication. In addition, during the anonymous authentication process, the session key can be negotiated for subsequent secure communication. The protocol is designed based on the identity cryptosystem, which does not need complex certificate management. The performance evaluation shows that this protocol can be effectively deployed in intelligent vehicle application scenarios with highly sensitive information.

Key words: intelligent vehicular ad hoc networks; identity anonymity; key exchange; two-way authentication; message authentication code

^{*} 收稿日期: 2023-02-16; 修回日期: 2023-06-02

基金项目: 国家自然科学基金(61902327); 中国博士后科学基金(2020M681316); 成都市科技局项目(2021-YF05-00965-SN); 西南石油大学高等教育教学改革研究项目(X2021JGZDI028)

通信地址: 610500 四川省成都市新都区新都大道 8 号西南石油大学计算机科学学院

Address: School of Computer Science, Southwest Petroleum University, 8 Xindu Avenue, Xindu District, Chengdu 610500, Sichuan, P. R. China

1 引言

智能车载网络 VANET (Vehicle Ad-hoc Network) 作为物联网在智能交通领域的重要应用^[1], 可以通过实现特殊车辆避让、碰撞预警等功能来帮助减轻交通压力, 减少交通事故, 提高交通运输效率和道路安全性, 因而受到工业界和学术界的广泛关注。

智能车载网络架构模型主要包括 3 类通信实体^[2,3]: 完全可信的第三方权威机构 TA (Trusted Authority)、车载通信单元 OBU (On Board Unit) 和路边基站单元 RSU (Road Side Unit)。其中可信机构 TA 负责维护整个系统, 结合应用服务器来计算发行系统公开参数, 可以广播交通预警等。通过车载通信单元 OBU 来实现智能车辆节点之间的实时信息交互, 如异常车辆状态预警、慢减速车辆预警等。通过实时信息交互可以有效减少交通事故的发生, 大大提高交通效率, 这种通信称为 V2V (Vehicle to Vehicle) 通信。车辆节点可以与路边基站单元 RSU 进行信息共享, 即 V2R (Vehicle to RSU) 通信^[4-7]。路边基站单元 RSU 是部署在道路两侧的基础设施, 可以和车辆节点进行通信完成实时信息交互, 即 R2V (RSU to Vehicle) 通信。信息交互时, RSU 会验证 OBU 发出的信息是否真实, 如果遇到紧急情况, RSU 可以直接向 TA 发送经验证的信息, 保证 TA 及时发出交通预警, 减少交通事故的发生, 同时也减轻了 TA 的负担。V2V、V2R、R2V 模式均使用专用短程通信技术 DSRC (Dedicated Short Range Communications) 进行通信。

网络的开放性和脆弱性使智能车载网络容易遭受各种安全攻击^[8-10], 进而导致交通事故的发生, 对人们的生命财产安全造成威胁。比如, 恶意车辆可能会伪装成紧急车辆进行危险操作, 也可能发布一些关于交通事故的假消息等。因此, 车辆节点在加入车联网并能在其中与其他合法车辆或 RSU 通信时, 必须先通过身份认证^[11,12]。同时, 一个安全的 VANET 还需要具有前向安全性、数据机密性, 并能抵抗常见的攻击, 如重放攻击。

在遭受网络攻击时, 用户个人隐私数据极有可能泄露, 这将会对用户造成极大的困扰, 且对智能车载网络的推广应用也十分不利。所以, 需要确保身份隐私性, 即任何其他车辆和路边基站单元都不能获取到车辆的真实身份信息^[13-15]。为了保证车

辆和附近 RSU 可以安全保密地通信, 还要求签订一个会话密钥交换协议。

近年来, 基于椭圆曲线加密和双线性对算法的认证方案已经广泛应用在智能车载网络领域。Wei 等^[16]和 Zhang 等^[17]基于椭圆曲线加密 ECC (Elliptic Curve Cryptography) 和 Shamir 门限技术提出了群组成员保护通信密钥的方案, 以较低的通信开销保护交通紧急消息的安全。文献^[18,19]也提出了解决用户隐私保护的匿名认证方案及无证书密码体制。Xiong 等^[20]提出了一种基于中国剩余定理 CRT (Chinese Remainder Theorem) 的具有动态隶属资格的条件隐私保护认证方法, RSU 可以同时验证大量接收到的消息, 从而提升了验证效率。文献^[21]提出了一种基于无证书密码和椭圆曲线密码的无证书条件隐私保护认证方案, 用于 VANET 中的安全车辆和基础设施通信。Song 等^[22]提出了一种基于双线性配对的智能车载网络条件隐私保护认证方案, 该方案采用路边单元中的防篡改装置与车辆一起完成信息签名和认证。

本文提出了适用于智能车载网络环境下的匿名认证与密钥交换协议, 已经匿名化处理过的车辆可以匿名向附近的 RSU 发送身份认证信息, 当 RSU 通过认证之后, 计算出一个消息认证码作为响应信息发送给请求认证车辆, 以实现双向认证, 进而防止恶意 RSU 的攻击。此外, 在匿名认证的同时还能进行会话密钥的协商, 以用于后续的安全保密通信。

2 预备知识

2.1 双线性对映射

G_1 是一个生成元为 P 的 q 阶加法循环群, 其中 q 为安全素数。 G_2 是一个 q 阶乘法循环群, 双线性对映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足以下 3 个性质:

(1) 双线性: 对于 $\forall Q, R \in G_1, \forall a, b \in \mathbf{Z}_q^*, e(aQ, bR) = e(abQ, R) = ab \cdot e(Q, R) = e(Q, R)^{ab}$;

(2) 非退化性: $\exists Q, R \in G_1$, 使得 $e(Q, R) \neq 1$;

(3) 可计算性: 对于 $\forall Q, R \in G_1$, 存在多项式时间算法能计算出 $e(Q, R)$ 。

2.2 系统网络模型与安全需求

智能车载网络中匿名认证与密钥交换协议的

系统网络模型(见图 1)包含 3 种通信实体:可信中心 TA、路边基站单元 RSU 和车载单元 OBU。下面分别对这 3 类通信实体进行介绍:

(1)可信中心 TA。TA 可作为智慧交通管理中心,是一个完全可信的第三方机构,具有高存储和高计算能力,主要为系统颁布公开参数,为 RSU 分配公私钥,以及为智能车辆生成私钥和注册信息。

(2)路边基站单元 RSU。RSU 是固定在道路两侧的信息基础设施,可以与智能车辆进行双向可认证保密通信。

(3)智能车载单元 OBU。OBU 使智能车辆可以和附近的 RSU 或智能车辆进行通信,可以与 RSU 进行相互认证以及密钥交换。

在开放的网络环境下,攻击者可通过窃听攻击、恶意追溯攻击来获取节点之间传输的消息,这极可能造成用户身份隐私和相关重要信息泄露的问题。此外,攻击者也可通过篡改、伪造、重放攻击造成重大交通事故,对人身安全造成威胁。因此,基于智能车载网络场景提出的协议需要满足以下安全特性:

(1)身份匿名性:任何其他车辆或 RSU 不能从窃听到的消息中获得车辆的真实身份信息,在某些场景下需要实现绝对匿名。

(2)身份认证:智能车载网络场景的有效实施必须保证节点间能相互认证,即保证通信双方的身份真实性,避免伪造、篡改攻击。

(3)认证密钥交换:对于智能车载网络场景中

有保密需求的数据,要保证其无法被未经授权的第三方知晓信息内容。为保证车载网络中数据传输的机密性,车辆和 RSU 需要在安全通信前完成会话密钥交换。

3 智能车载协议

3.1 协议具体设计

智能车载网络中匿名认证与密钥交换协议主要包括 4 个阶段:系统初始化、智能车辆注册、匿名认证、认证密钥交换。

(1)系统初始化阶段。可信中心 TA 通过以下步骤生成系统公开参数:

①TA 选取 2 个安全素数 p, q , 设置定义在 $y^2 = x^3 + ax + b \bmod p$ 上的非奇异椭圆曲线 E 。TA 选取一个生成元为 P 的 q 阶加法循环群 G_1 , 构造一个双线性对映射 $e: G_1 \times G_1 \rightarrow G_2$, 其中 G_2 是一个 q 阶乘法循环群。

②TA 选取一个随机数 $sk \leftarrow \mathbb{Z}_q^*$ 作为它的私钥,然后计算其公钥 $P_{pub} = skP$ 。

③TA 设置安全哈希函数, $H_1: \{0, 1\}^* \rightarrow G_1$, $H_2: G_2 \times \{0, 1\}^* \rightarrow \mathbb{Z}_q$, $h_1: G_1 \times \{0, 1\}^* \times G_1 \rightarrow \mathbb{Z}_q$, $h_2: G_1 \times G_1 \rightarrow \{0, 1\}^l$, 其中 l 为会话密钥长度。

④TA 选取一个消息认证码函数 MAC。最后,TA 输出系统公开参数 $P_{ara} = (E, p, q, P, P_{pub}, H_1, H_2, h_1, h_2, MAC)$, 然后将其预加载到所有智能车辆的防篡改装置中,并发送给所有路边基

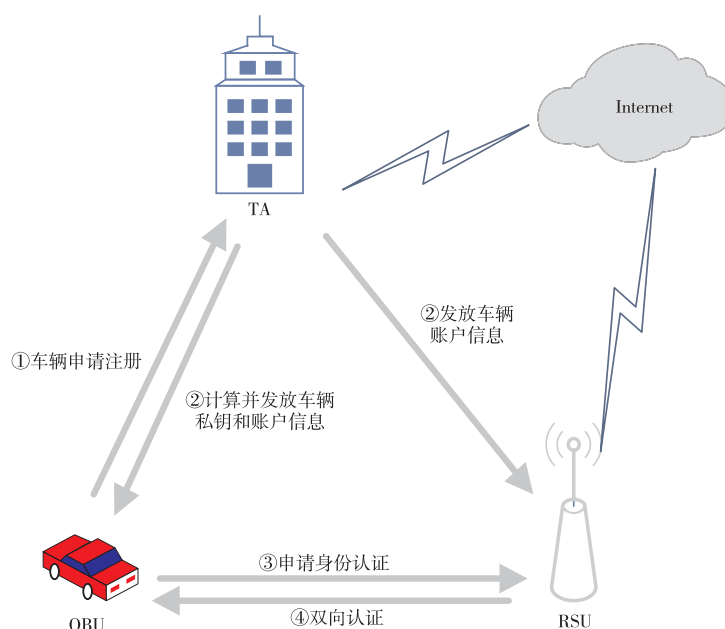


Figure 1 System network model

图 1 系统网络模型

站单元 RSU。此外,系统为每一个路边基站单元 RSU_j 设置一个长期有效的公私钥对 (sk_{RSU_j}, Q_{RSU_j}) ,其中私钥 $sk_{RSU_j} \leftarrow \mathbf{Z}_q^*$,公钥 $Q_{RSU_j} = sk_{RSU_j} P$ 。

(2)智能车辆注册阶段。在此阶段,智能车辆 V 需要向可信中心 TA 进行注册,以便安全地和附近的 RSU 进行信息交互。首先,智能车辆会将其真实的身份信息 ID_V 发送给 TA 以请求进行注册,如果身份信息不合法则拒绝注册请求。如果身份信息合法,则 TA 以密钥生成中心 KGC (Key Generation Center) 的角色为申请注册的智能车辆生成对应私钥和相应的注册信息。具体注册操作步骤如下所示:

①TA 为申请注册的智能车辆 V 计算其私钥 $SK_{ID_V} = sk H_1(ID_V)$ 。

②TA 为智能车辆计算一个身份标识符 $Index_{ID_V} = e(H_1(ID_V), P_{pub})$,这个身份标识符可作为智能车辆的匿名身份信息,与智能车辆真实身份信息 ID_V 一一对应,且只由 ID_V 决定。

③TA 为智能车辆计算注册状态信息索引号 $S = H_2(Index_{ID_V} \parallel aux)P$,其中 aux 为附加信息,如服务类型、注册信息有效期等。在后续验证阶段,RSU 可根据此索引号在数据库中查找智能车辆注册信息以进行验证。

最后,TA 通过安全信道将私钥和注册信息 $(SK_{ID_V}, S, Index_{ID_V}, aux)$ 发送给申请注册的智能车辆,并通过安全信道将智能车辆的注册信息 $(S, Index_{ID_V}, aux)$ 发送给附近所有的路边单元 RSU,然后 RSU 将此智能车辆注册信息保存到后台数据库。

(3)匿名认证阶段。在此阶段,身份已经匿名的智能车辆 V 向附近的路边基站单元 RSU 申请身份认证并发送认证请求消息。具体计算过程如下所示:

①智能车辆选择随机数 $x \leftarrow \mathbf{Z}_q^*$,并计算 $W = xP, W' = xQ_{RSU}$ 以及 $S' = S + W$ 。

②选取一个认证序列号 $nonce \in \{0,1\}^*$,计算认证符 $\delta = (h_1(S \parallel nonce \parallel Q_{RSU}) + x)^{-1} SK_{ID_V}$ 。

③计算会话密钥 $K = h_2(W \parallel W')$ 。

最后,申请认证的智能车辆 ID_V 将认证请求信息 $Auth = (\delta, nonce, W', S')$ 发送给附近的路边基站单元 RSU。

(4)认证密钥交换阶段。在这个阶段,当接收到认证请求信息 $Auth = (\delta, nonce, W', S')$ 时,RSU 将会进行一系列操作来完成对智能车辆的认证以及密钥的协商。具体过程如下所示:

①RSU 用自己的私钥来计算 $W = sk_{RSU}^{-1} W'$ 并恢复智能车辆的状态信息索引号 $S = S' - W$ 。

②RSU 在数据库中根据恢复出的注册状态信息索引号 S 定位身份标识符 $Index_{ID_V}$,并验证等式 $Index_{ID_V} = e(\delta, h_1(S \parallel nonce \parallel Q_{RSU})P + W)$ 是否成立。

③如果等式成立,则计算会话密钥 $K = h_2(W \parallel W')$ 。

④RSU 利用消息认证码函数 MAC 计算 $MAC_K(\delta \parallel nonce + 1)$ 作为响应信息发送给请求认证的智能车辆。

智能车辆一旦接收到从附近 RSU 发出的响应信息 $MAC_K(\delta \parallel nonce + 1)$,就使用会话密钥 K 计算出消息认证码进行比对。如果计算结果相同,则表示智能车辆可以以匿名的方式与附近 RSU 实现身份认证与密钥协商功能,并且后续可以安全地和附近 RSU 进行通信。若计算结果不同,则重启协议。

3.2 协议的正确性

协议中通过 RSU 的私钥恢复 W ,恢复过程是 $W = sk_{RSU}^{-1} W' = sk_{RSU}^{-1} x Q_{RSU} = sk_{RSU}^{-1} x sk_{RSU} P = xP$ 。由于双线性对映射具有双线性、非退化性和可计算性,故 RSU 可利用已知信息通过验证等式 $Index_{ID_V} = e(\delta, h_1(S \parallel nonce \parallel Q_{RSU})P + W)$ 是否成立来判断身份认证成功与否,正确性推导如下所示:

$$\begin{aligned} e(\delta, h_1(S \parallel nonce \parallel Q_{RSU})P + W) &= e((h_1(S \parallel nonce \parallel Q_{RSU}) + x)^{-1} SK_{ID_V}, h_1(S \parallel nonce \parallel Q_{RSU})P + W) \\ &= e((h_1(S \parallel nonce \parallel Q_{RSU}) + x)^{-1} sk H_1(ID_V), h_1(S \parallel nonce \parallel Q_{RSU})P + xP) \\ &= e((h_1(S \parallel nonce \parallel Q_{RSU}) + x)^{-1} sk H_1(ID_V), (h_1(S \parallel nonce \parallel Q_{RSU}) + x)P) \\ &= e(H_1(ID_V), P_{pub}) = Index_{ID_V} \end{aligned}$$

4 安全性分析

协议安全性分析需要证明该协议具有身份的匿名性与可认证性,并具有认证密钥交换的功能。

定理 1 基于智能车载网络的匿名认证与密钥交换协议满足身份的完全匿名性以及可认证性。

在匿名认证阶段,智能车辆发送认证请求信息 $Auth = (\delta, nonce, W', S')$ 给附近的路边基站单元 RSU。RSU 在接收到此请求后,首先使用自己的私钥 sk_{RSU} 计算出 $W = sk_{RSU}^{-1} W'$,进而恢复出注册

状态信息索引号 $S = S' - W$, 然后在后台数据库中根据 S 定位身份标识符 $Index_{ID_V}$ 。RSU 可以通过验证等式 $Index_{ID_V} = e(\delta, h_1(S \parallel nonce \parallel Q_{RSU})P + W)$ 是否成立来判断身份认证成功与否。根据离散对数困难问题假设, 如果不知道 RSU 的私钥, 那么攻击者是不可能恢复出 W 的, 也不可能成功伪造一个能通过验证方程的 $Index_{ID_V}$ 。即使攻击者和 RSU 知道 $Index_{ID_V}$, 但由于智能车辆真实身份 ID_V 被隐藏在了双线性对映射 $Index_{ID_V} = e(H_1(ID_V), P_{pub})$ 中, 所以智能车辆的真实身份能保证完全匿名。同时, $\delta = (h_1(S \parallel nonce \parallel Q_{RSU}) + x)^{-1} SK_{ID_V}$ 是一个基于身份的数字签名, 如果没有对应的私钥 SK_{ID_V} , 则无法成功伪造出一个能够通过验证方程 $Index_{ID_V} = e(\delta^*, h_1(S^* \parallel nonce \parallel Q_{RSU})P + W)$ 的数字签名 $\delta^* = (h_1^*(S^* \parallel nonce \parallel Q_{RSU}) + x)^{-1} SK_{ID_V}$ 。

因此, 基于智能车载网络的匿名认证与密钥交换协议满足身份的匿名性和可认证性。

定理 2 基于智能车载网络的匿名认证与密钥交换协议可实现可验证的密钥交换功能。

在本文协议中, 只有使用私钥 sk_{RSU} 才能恢复出 $W = sk_{RSU}^{-1} W'$, 所以 W 在智能车辆和 RSU 之间都是安全的, 所以会话密钥 $K = h_2(W \parallel W')$ 可以在智能车辆和 RSU 之间安全共享。当 RSU 对请求认证车辆认证成功后, 便可以确定会话密钥 K , 然后通过会话密钥计算出 $MAC_K(\delta \parallel nonce + 1)$ 作为响应信息发送给请求认证的智能车辆。此时, 智能车辆就会使用密钥 K 计算出消息认证码来与之进行比对。如果结果相同, 则表明智能车辆确定接收此密钥为会话密钥, 而且以后也可以通过 K 安全地和附近 RSU 进行通信, 确保了消息的机密性。故本文协议可以实现智能车辆和附近 RSU 的可验证密钥交换功能, 同时可以抵抗中间人攻击。如果攻击者想要获得此会话密钥, 只有通过离线猜测攻击这种方式。但是, 由于消息认证码具有抗碰撞的特性, 想要构造出 $MAC_{K^*}(\delta \parallel nonce + 1)$ 和 $MAC_K(\delta \parallel nonce + 1)$ 相等的结果在计算上是不可行的。此外, 本文协议中还嵌入了认证序列号 $nonce$, 可以抵抗重放攻击。

5 性能对比与分析

5.1 计算开销分析

本节将基于智能车载网络的匿名认证与密钥

交换协议与基于双线性对映射设计的文献[23]中协议、APKI 协议^[24]和 EAAP 协议^[25]进行计算开销分析与比较。协议中所有算法的实现环境为: Windows 10 操作系统, Intel® Core™ i5-2320 3.0 GHz 处理器, 8 GB 内存。所有算法都使用 C 语言的版本号为 5.6.2 密码算法基础函数库 MIRACL 实现, 为了后续可以更方便地进行计算开销分析, 用符号 *Pair*, *Exp*, *Mult*, *mult*, *Hash*, *hash*, *Add*, *Inv* 和 *Exp* 来分别表示双线性对运算时间、普通模指数运算时间、椭圆曲线中的倍点运算时间、普通模乘法运算时间、映射到循环群中的哈希运算时间、普通哈希运算时间和椭圆曲线上的加法运算时间、模逆运算时间和双线性对幂运算时间, 以及用符号 *Mac* 表示计算消息认证码的运算时间。

在文献[23]中, 分析得知当车辆进入一个 RSU 通信范围之前, 车辆需要提前获取 TA 颁发的混淆值和伪身份列表, 并基于每一个伪身份列表和已知参数生成特定点后将认证消息发送给 RSU。在此过程中, 车辆需要执行 3 次普通哈希运算以确保完整性, 然后执行 2 次倍点运算和 1 次双线性对幂运算来生成智能车辆签名。因此, 智能车辆的计算开销为 $3hash + 2Mult + Exp$ 。而 RSU 在接收到其通信范围内的车辆发送的认证请求后, 需要执行 1 次双线性对运算、2 次普通哈希运算和 1 次双线性对幂运算运算验证车辆身份。因此, RSU 总的计算开销为 $Pair + 2hash + Exp$ 。

对 APKI 协议^[24]分析得知, RSU 生成广播签名给附近需要认证的智能车辆, 智能车辆收到后执行 1 次普通哈希运算和 1 次双线性对运算验证 RSU 的合法性。智能车辆通过执行 4 次倍点运算和 1 次普通哈希运算生成签名, 所以智能车辆端总的计算开销为 $Pair + 4Mult + 2hash$ 。RSU 收到认证请求后执行 1 次普通哈希运算验证其完整性, 执行 2 次双线性对运算、2 次倍点运算和 2 次普通哈希运算完成签名消息的认证, 因此 RSU 总的计算开销为 $2Pair + 2Mult + 2hash$ 。

对 EAAP 协议^[25]分析得知, 智能车辆需要执行 6 次模指数运算、1 次普通模乘法运算、3 次椭圆曲线上的加法运算、1 次普通哈希运算和 1 次逆运算得到匿名证书, 然后执行 1 次模指数运算、1 次普通哈希运算、1 次逆运算和 1 次椭圆曲线上的加法运算得到签名信息, 并最终发送给 TA 进行验证, 在此方案中 TA 相当于本文方案的 RSU。因此, 智能车辆的计算开销为 $7Exp + mult + 4Add +$

$2hash + 2Inv$ 。当接收到验证信息后,接收方执行 4 次普通模乘法运算、7 次模指数运算、2 次逆运算、2 次普通哈希运算和 2 次双线性对运算完成验证。因此,接收方的计算开销为 $4mult + 7Exp + 2Inv + 2hash + 2Pair$ 。

在本文协议中,车辆需要执行 2 次倍点运算得到 W 和 W' ,执行 1 次椭圆曲线上的加法运算得到 S' 。然后执行 1 次倍点运算、1 次普通哈希运算和 1 次逆运算得到签名 δ 。最后再执行 1 次普通哈希运算得到会话密钥 K 。因此,智能车辆在计算认证消息时总的计算开销为 $3Mult + Add + 2hash + Inv$ 。当 RSU 对智能车辆进行认证时,需要执行 1 次倍点运算和 1 次逆运算得到 W ,再执行 1 次椭圆曲线上的加法运算得到智能车辆注册状态信息索引号 S 。然后执行 1 次椭圆曲线上的加法运算、1 次倍点运算、1 次双线性对运算和 1 次普通哈希运算来验证认证等式 $Index_{ID_V} = e(\delta, h_1(S \parallel nonce \parallel Q_{RSU})P + W)$ 是否成立。再执行 1 次普通哈希运算完成会话密钥 K 的交换。最后,执行 1 次消息认证码运算完成智能车辆和 RSU 的双向认证。因此 RSU 的认证计算开销总共为 $2Mult + Inv + 2Add + Pair + 2hash + Mac$ 。

从图 2 可以看出,与文献[23]中协议、APKI 协议和 EAAP 协议相比,本文提出的基于智能车载网络的匿名认证与密钥交换协议在智能车辆和路边基站单元方面都具有更低的计算开销,因此本文设计协议在智能车载网络环境具有明显的计算性能优势。

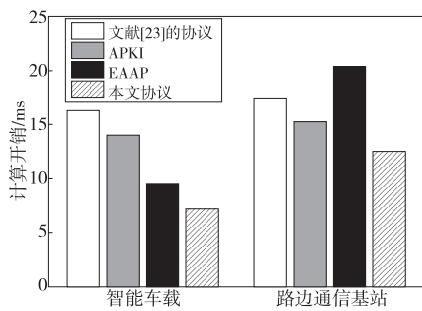


Figure 2 Comparison of computational costs

图 2 计算开销比较

5.2 通信开销分析

本节对智能车辆和 RSU 进行双向认证时产生的通信开销进行分析与比较。首先统一循环群中的元素长度为 1 024 bit,用 $|G|$ 表示。将 $nonce$ 和 PID 长度固定为 32 bit,用符号 ξ 表示。统一 Z_q 中的元素长度为 160 bit,用 $|q|$ 表示。将时间戳和假名过期时间都设置为 32 bit,分别用

$|ts|$ 和 $|ex|$ 表示。

在基于智能车载网络的匿名认证与密钥交换协议中,通信开销主要来自车辆发送认证请求信息给 RSU,以便完成车辆和 RSU 的双向认证。在匿名认证阶段,车辆上传单个认证请求信息 $Auth = (\delta, nonce, W', S')$ 到 RSU 的通信开销为 $3|G| + \xi = 3104$ bit,如果 n 个车辆上传 n 个认证请求消息,则通信开销为 $3n|G| + n\xi = 3104n$ bit。

文献[23]的协议中,在认证前车辆生成签名 $\sigma = (C, L, K, T, R, f(PID_{b,n}))$,其中, C 为消息加密值, L 为伪身份列表, K 为基于随机数生成的点, T 为当前时间戳, R 为基于伪身份生成对应循环群中的若干点。用伪身份列表以环信号方式构建签名,会涉及较大的通信开销,函数 $f(PID_{b,n})$ 长度用 1 bit 表示。因此,智能车辆通信开销为 $2|G| + 6|G_T| + 6|PID| + |ts| + |f(PID)| = 8417$ bit, n 个车辆的通信开销为 $8417n$ bit。

在 APKI 协议^[24]中,智能车辆和 RSU 进行相互认证时,RSU 和智能车辆都会发送认证信息给对方。智能车辆将接收 RSU 的广播消息并验证其合法性,RSU 的通信开销为 $3|q| + |ts| + |G| = 1536$ bit。智能车辆基于多方公钥生成签名并发送给 RSU 的开销为 $4|G| + 2|q| + |ts| = 4448$ bit,智能车辆进行一次认证总的通信开销为 $5|G| + 5|q| + 2|ts| = 5984$ bit。RSU 以广播的形式与智能车辆进行验证,因此 n 辆车的通信开销为 $(4n+1)|G| + (2n+3)|q| + (n+1)|ts| = (4448n+1536)$ bit。在 EAAP 协议^[25]中,TA 充当了本文协议中 RSU 的角色,当智能车辆向 TA 认证时,智能车辆发送认证信息给 TA 的通信开销为 $2|G| = 2048$ bit,如果有 n 辆车需要认证,则通信开销将为 $2n|G| = 2048n$ bit。

从图 3 可以看出,本文提出的基于智能车载网络的匿名认证与密钥交换协议比文献[23]中的协议和 APKI 协议的通信开销低。虽然 EAAP 协议的通信开销比本文协议的略低,但本文协议能够有效实现双向认证功能。由数据分析得知,在智能车辆数到达 500 时,文献[23]中的协议和 APKI 协议的通信开销约为本文协议的 1.5 倍以上,且随着智能车载数量的增加,本文协议的通信开销优势将更为明显。

6 结束语

本文提出了一个适用于智能车载网络的匿名

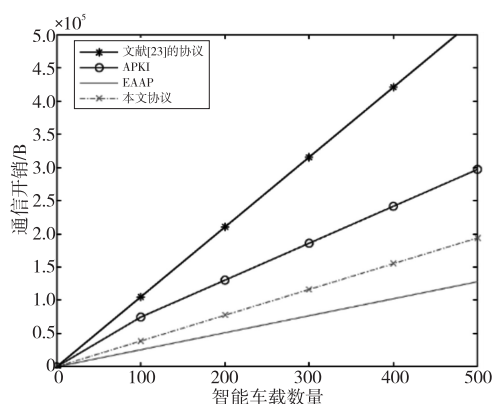


Figure 3 Comparison of communication overhead

图3 通信开销比较

认证与密钥交换协议,实现了智能车辆以完全匿名的方式与附近的RSU进行双向认证以及会话密钥的交换。安全性分析表明,本文协议可以有效确保身份的匿名性与可认证性,可实现可验证的密钥协商功能。性能比较与分析的结果表明,本文设计的协议具有轻量级的性能优势,这对于移动智能车载通信场景的应用具有实际意义。

参考文献:

- [1] Borcoci E, Drăgulescu A M, Li F Y, et al. An overview of 5G slicing operational business models for internet of vehicles, maritime IoT applications and connectivity solutions[J]. IEEE Access, 2021, 9: 156624-156646.
- [2] Din S, Paul A, Rehman A. 5G-enabled hierarchical architecture for software-defined intelligent transportation system[J]. Computer Networks, 2019, 150: 81-89.
- [3] 张毅, 姚丹亚, 李力, 等. 智能车路协同系统关键技术与应用[J]. 交通运输系统工程与信息, 2021, 21(5): 40-51.
Zhang Yi, Yao Dan-ya, Li Li, et al. Technologies and applications for intelligent vehicle-infrastructure cooperation systems[J]. Journal of Transportation Systems Engineering and Information Technology, 2021, 21(5): 40-51.
- [4] Ghafoor K Z, Guizani M, Kong L, et al. Enabling efficient co-existence of DSRC and C-V2X in vehicular networks[J]. IEEE Wireless Communications, 2019, 27(2): 134-140.
- [5] Jiang D, Delgrossi L. IEEE 802. 11 p: Towards an international standard for wireless access in vehicular environments [C]//Proc of VTC Spring 2008-IEEE Vehicular Technology Conference, 2008: 2036-2040.
- [6] Kiela K, Barzdenas V, Jurgo M, et al. Review of V2X-IoT standards and frameworks for ITS applications[J]. Applied Sciences, 2020, 10(12): 4314.
- [7] Naik G, Choudhury B, Park J M. IEEE 802. 11 bd & 5G NR V2X: Evolution of radio access technologies for V2X communications[J]. IEEE Access, 2019, 7: 70169-70184.
- [8] 徐猛, 刘涛, 钟绍鹏, 等. 城市智慧公交研究综述与展望[J]. 交通运输系统工程与信息, 2022, 22(2): 91-108.
Xu Meng, Liu Tao, Zhong Shao-peng, et al. Urban smart pub-

lic transport studies: A review and prospect[J]. Journal of Transportation Systems Engineering and Information Technology, 2022, 22(2): 91-108.

- [9] Kelarestaghi K B, Foruhandeh M, Heaslip K, et al. Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures[J]. arXiv: 1903. 01541, 2019.
- [10] Khelifi H, Luo S, Nour B, et al. Named data networking in vehicular ad hoc networks: State-of-the-art and challenges [J]. IEEE Communications Surveys & Tutorials, 2019, 22 (1): 320-351.
- [11] Cunha F, Villas L, Boukerche A, et al. Data communication in VANETs: Protocols, applications and challenges[J]. Ad Hoc Networks, 2016, 44: 90-103.
- [12] Mansour M B, Salama C, Mohamed H K, et al. VANET security and privacy—An overview[J]. International Journal of Network Security & Its Applications, 2018, 10(2): 13-34.
- [13] Choi H K, Kim I H, Yoo J C. Secure and efficient protocol for vehicular ad hoc network with privacy preservation[J]. EURASIP Journal on Wireless Communications and Networking, 2011, 2011(1): 716794.
- [14] Mohanty S, Jena D. Secure data aggregation in vehicular-adhoc networks: A survey[J]. Procedia Technology, 2012, 6: 922-929.
- [15] Allani S, Yeferny T, Chbeir R, et al. Towards a smarter directional data aggregation in VANETs[J]. World Wide Web, 2020, 23(4): 2303-2322.
- [16] Wei L, Cui J, Xu Y, et al. Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs[J]. IEEE Transactions on Information Forensics and Security, 2020, 16: 1681-1695.
- [17] Zhang J H, Zhang Q J. Comment on secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs[J]. IEEE Transactions on Information Forensics and Security, 2021, 18: 1037-1038.
- [18] 丁宾宾, 曹素珍, 丁晓晖, 等. 基于身份的无对密文等值测试公钥加密方案[J]. 计算机工程与科学, 2022, 44(12): 2146-2152.
Ding Bin-bin, Cao Su-zhen, Ding Xiao-hui, et al. Pairing-free identity-based public key encryption with equality test[J]. Computer Engineering & Science, 2022, 44 (12): 2146-2152.
- [19] 寇邦艳, 曹素珍, 吕佳. 基于雾计算面向停车服务的隐私保护方案[J]. 计算机工程与科学, 2022, 44(7): 1232-1238.
Kou Bang-yan, Cao Su-zhen, Lü Jia. A privacy protection scheme for parking services based on fog computing[J]. Computer Engineering & Science, 2022, 44(7): 1232-1238.
- [20] Xiong H, Chen J, Mei Q, et al. Conditional privacy-preserving authentication protocol with dynamic membership updating for VANETs[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(3): 2089-2104.
- [21] Ji S, Gui Z, Zhou T, et al. An efficient and certificateless conditional privacy-preserving authentication scheme for

wireless body area networks big data services[J]. IEEE Access, 2018, 6: 69603-69611.

- [22] Song C, Gu X A, Ping Y, et al. Conditional privacy protection authentication scheme based on bilinear pairings for VANET[J]. The Journal of China Universities of Posts and Telecommunications, 2020, 27(1): 62-71.
- [23] Luo M, Zhou Y. An efficient conditional privacy-preserving authentication protocol based on generalized ring signcryption for VANETs [J]. IEEE Transactions on Vehicular Technology, 2022, 71(9): 10001-10015.
- [24] Jiang S, Chen X, Cao Y, et al. APKI: An anonymous authentication scheme based on PKI for VANET[C]//Proc of 2022 7th International Conference on Computer and Communication Systems, 2022: 530-536.
- [25] Azees M, Vijayakumar P, Deboarh L J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(9): 2467-2476.

作者简介:



张晓均(1985-),男,四川成都人,副教授,研究方向为密码学与信息安全。E-mail: zhangxjdzk2012@163.com

ZHANG Xiao-jun, born in 1985, associate professor, his research interest includes

cryptography & information security.



唐浩宇(1999-),男,四川眉山人,硕士生,研究方向为密码学与信息安全和车联网安全。E-mail: tanghaoyu35@gmail.com

TANG Hao-yu, born in 1999, MS candidate, his research interests include cryptography & information security and Internet of vehicles security.



付红(1996-),女,四川眉山人,硕士生,研究方向为车联网安全。E-mail: 1157501262@qq.com

FU Hong, born in 1996, MS candidate, her research interest includes Internet of vehicles security.



王文琛(1997-),男,天津人,硕士生,研究方向为车联网安全。E-mail: wenchen_1009@163.com

WANG Wen-chen, born in 1997, MS candidate, his research interest includes Internet of vehicle security.

《计算机工程与科学》征文通知

《计算机工程与科学》是由国防科技大学计算机学院主办的中国计算机学会会刊,是国内外公开发行的计算机类综合性学术刊物,现为月刊。

本刊欢迎关于高性能计算、计算机科学理论、计算机组织与系统结构、计算机软件、计算机网络与信息安全、计算机器件设备与工艺等学科领域方面的来稿。

本刊常年设有高性能计算专栏。

来稿论文必须未发表、未投到其他会议或期刊。

来稿要求和注意事项:

(1) 主题明确、文字精练、语句通顺、数据可靠。

(2) 标题、作者单位、摘要、关键词采用中英文间隔行文;请注明是否基金资助项目论文(注明项目名称和编号),并注明文章中图法分类号。务必附上所有作者中英文简历(姓名、性别、出生年月、籍贯、学位、职称、研究方向)、1寸证件照片(军人请用便服照)、中英文通信地址、联系电话和 Email。

(3) 作者在投稿时须注明是否是 CCF 会员(高级会员、普通会员、学生会会员),若是会员,请注明会员号。

(4) 来稿请用 WORD 软件编辑,格式为 A4, 40 行×40 列,通栏排版,正文为 5 号宋体,论文长度不得低于 6 个标准版面,并请自留底稿。

(5) 来稿中图形绘制要求工整、清晰、紧凑,尺寸要适当,图中文字用 6 号宋体,线为 0.5 磅。

(6) 每篇论文格式要求:1 引言;……;最后是结束语。引言和结束语中尽量不用图和表。附录应放参考文献之后。参考文献限已公开发表的。

(7) 来稿文责自负,要遵守职业道德,如摘引他人作品,务请在参考文献中予以著录。署名的作者应为参与创作,对内容负责的人。文章发表后,如不同意其他报、刊、数据库等转载、摘编其作品,请在来稿时声明。

(8) 本刊不收取作者任何费用(免审稿费、版面费等所有费用)。

联系地址:410073 湖南省长沙市国防科技大学《计算机工程与科学》编辑部

联系电话:0731-87002567

电子邮箱:jsjgcykx@vip.163.com

投稿主页: <http://joces.nudt.edu.cn>